UNIVERSIDAD
DE SANTIAGO
DE CHILE

Departamento de Matemática y Ciencia de la Computación

Laboratorio 2

AES: Advanced Encryption Standard

Primer Semestre 2018

Criptografía 22633
Licenciatura en Ciencia de la Computación

Gustavo Rojas Torres
gustavo.rojas.t@usach.cl

1 Introducción

El objetivo de este trabajo es análizar e implementar la primera ronda del algoritmo de encriptación AES.

2 Algoritmo implementado

El algoritmo para obtener la fila y columna de cada bloque A de 8 bits.

function row-and-column
precondition: array[] arreglo A de bits, arrayn[] arreglo para las nuevas posiciones en PC-1
postcondition: Arreglo con las especificaciones de filas y columnas

```
1  begin function
2      j←0
3      for i← 0 to n do
4          row_j = array_i*8 + array_i + 1*4 + array_i + 2*2 + array_i + 3*1
5          column_j = array_i + 4*8 + array_i + 5*4 + array_i + 6*2 + array_i + 7*1
6          j←j+1
7      end for
8  end function
```

El algoritmo para convertir binarios a hexadecimal.

function bintohex
precondition: hex[] arreglo vacío
postcondition: Arreglo hex[] de hexadecimales.

```
1  begin function
2      for i←0 to 16 do
3          hex[i] = SBox[row[i]][column[i]]
4      end for
6  end function
```

El algoritmo para mostrar el hexadecimal como binario.

function hextobin
precondition: hex[] arreglo de hexadecimales
postcondition: Representación binaria de cada hexadecimal

```
1   begin function
2       for i←0 to 16 do
3           for pb←7 to 0 do
4               if hex_i and (1 << pb))
5                   print 1
6               else
7                   print 0
8           end for
9       end for
10      print |
11  end function
```

3 Formulación del experimento

Los requisitos que debe cumplir este nuevo criptosistema son: Cifrado de bloque, con bloques de 128-bits. Debe soportar claves de longitud: 128, 192 y 256 bit.

Para poder obtener los resultados del algoritmo AES: Advances Encryption Standard, se implementó el algoritmo en lenguaje C.

4 Curvas de desempeño de resultados

```
1. 128 bits

Plaintext:
 00011001011100101110100010011000011111000110110001111110101100101000100000011101010000000010000100111011000110011010000001001111

Binarios convertidos a hexadecimal:
 D4|40|9B|46|10|50|F3|37|C4|A4|09|FD|E2|D4|E0|84|

Representacion binaria de los hexadecimales:
 11010100|01000000|10011011|01000110|00010000|01010000|11110011|00110111|11000100|10100100|00001001|11111101|11100010|11010100|11100000|10000100|

Primera Ronda del AES:
 00010000000100000011000000100000011100010110001111010010100100010010000000010000010000001100000000101100000110000001010000110100

Tiempo: 0.000728
```

5 Conclusiones

El AES: Advanced Encryption Standard es considerado un criptosistema más seguro, y es eficiente en software como en hardware, en comparación del DES el cual es un cryptosistema mucho menos seguro ya que en este se utilizan ocho diferentes S-Boxes, mientras que en el AES todos los 16 S-Boxes son idénticos.

6 Forma de Compilación

En la terminal, ubicarse en el directorio donde se encuentra el codigo.c

```
1 gcc lab2.c -o lab2
2 ./lab2
```